PCT/EP 00/08263

BUNDESREPUBLIK DEUTSCHLAND

09/830734

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

EP 00/08263

EU

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	199 41 550.1
Anmeldetag:	01. September 1999
Anmelder/Inhaber:	Deutsche Telekom AG, Bonn/DE
Bezeichnung:	Verfahren zur Freischaltung von kundenrelevanten Berechtigungen auf Sicherheitsmodulen in Conditional Access für Pay-Dienste
IPC:	H 04 L, H 04 N, G 07 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 20. Juli 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Verfahren zur Freischaltung von kundenrelevanten Berechtigungen auf Sicherheitsmodulen in Conditional Access Systemen für Pay-Dienste

Technisches Gebiet:

Die Erfindung betrifft ein Verfahren zur Freischaltung von kundenrelevanten Zugangsberechtigungen in Conditional Access-Systemen zum Empfang gebührenpflichtiger Dienste, wie Pay-TV, digitale Rundfunkdatendienste im DAB, DVB, Swift, Video-on-Demand sowie beliebiger digitaler Dienste, die über Rundfunksysteme ausgestrahlt werden, unter Benutzung von Sicherheitsmodulen, wie Smart Cards, auf welchen Sicherheitsalgorithmen und/oder kundenspezifische Berechtigungen in Form von Softwareprogrammen und Daten gespeichert sind, gemäß dem Oberbegriff des Anspruchs 1.

Stand der Technik:

Sicherheitsmodule in Form von Smart Cards werden heute bereits in vielen Bereichen eingesetzt, in denen es gilt, Personen oder auch Maschinen einen berechtigungs- oder bedingungsabhängigen Zugriff [Conditional Access (CA-Systeme)] auf Daten oder Programme oder weitere Maschinen zu gewähren, wenn die gesetzten Bedingungen oder Berechtigungen erfüllt sind (z.B. Pay-TV). Andere typische Einsatzbereiche für Smart Cards sind elektronische Zahlungsmittel, GSM-Telefonie oder digitale Rundfunkdatendienste im DAB, DVB, Swift wie auch künftig Video-on-Demand.

Die Zugriffssteuerung erfolgt in modernen Conditional Access-Systemen fast ausschließlich auf der Basis von Smart Cards in Chipkarten-Technologie. Diese Smart Cards enthalten einen gespeicherten Sicherheitsalgorithmus und kundenspezifische Berechtigungen zum Empfang kostenpflichtiger Datendienste.

Die Problemstellung für Conditional Access-Systeme besteht darin, daß ein Anbieter von Diensten, ein Content Provider, sicher mehr als einen Kunden, wiederum aber auch nicht alle erreichen möchte. Zum Empfang eines Dienstes sollen nur dazu autorisierte Kunden in der Lage sein. Dies sind solche Kunden, die bestimmte definierte Bedingungen durch den Kauf von Berechtigungen erfüllen, zum Beispiel, dass sie die monatliche Abonnementsgebühr bezahlt haben. Zur Übermittlung derartiger Berechtigungen werden Rundfunksysteme benutzt. Somit stellt sich das Problem, dass der Zugriff auf bestimmte über Rundfunksysteme verbreitete Informationen kontrolliert werden soll, die aber im Prinzip von jedermann empfangen werden können.

Die Zugriffssicherung derartiger Informationen, wie z.B. Pay-TV, mittels Conditional Access-Systemen geschieht durch Scrambling, das ist Verschlüsselung der Programminhalte, durch Speicherung von Empfangsberechtigungen im Sicherheitsmodul des Endgerätes, und durch Hinzufügen von Empfangsbedingungen zum Programm. Endgeräte zum Empfang eines Pay-TV-Programmes sind meist die sogenannten Set-Top-Boxen oder Dekoder. Es sind aber auch andere Endgeräte möglich, z.B. mobile Empfangsgeräte, PC-Karten oder PCMCIA-Module, oder das Endgerät kann in den Fernseher integriert sein. In vielen Fällen ist jedoch die Freischaltung von Smart Cards in Rundfunksystemen, besonders beim Einsatz in Geräten zum Mobilempfang von Diensten ohne Punkt zu Punkt-Verbindung wie beim Telefon, wegen der fehlenden Empfangsgarantie problematisch. Erst die Freischaltung ermöglicht es, dass ein Kunde direkt nach dem Erwerb einer Karte einen von ihm gewünschten Dienst nutzen kann. Der Absender einer Freischaltung hat jedoch meist keine Information darüber, ob seine Freischaltung auch tatsächlich beim Kunden angekommen ist. Eine Freischaltung kommt dann nicht zustande, wenn ein Rundfunkempfang für das benutzte Gerät unmöglich ist, z.B. durch Gebäudeabschirmung in Tiefgaragen oder z.B. in Fällen, in denen ein zum Aussenden von Berechtigungen erforderliches Funknetz noch nicht so weit ausgebaut ist, daß ein Empfang von Berechtigungen durch eine sogenannte EMM-Nachricht (Entitlement Management Messages) nicht flächendeckend möglich ist. Dem gegenüber ist eine kontrollierte

Erstfreischaltung mit Rückmeldung sehr sicher und ermöglicht zudem ein augenblickliches Inkasso für den freigeschalteten Dienst zum Zeitpunkt seines Erwerbs.

Programminhalte werden gescrambelt, indem die Daten von einem Verschlüsselungsalgorithmus unter Kontrolle eines sogenannten Kontrollwortes CW verschlüsselt werden. Als Algorithmus kommt im digitalen, auf dem MPEG-2-Standard basierenden Fernsehen, in Europa hauptsächlich der DVB Common Scrambling Algorithmus zum Einsatz. Es sind aber auch andere Algorithmen möglich, wie zum Beispiel DES oder Triple DES u.a. (vgl. Bruce Schneier, Angewandte Kryptographie, Wiley, 1996).

In sog. Entitlement Controll Messages (ECM) werden einem Dekoder oder sonstigem Empfangsmodul außer neuen Kontrollwörtern (CW) auch die Bedingungen mitgeteilt, unter denen ein Programm empfangen werden darf. Da sowohl das CW als auch die Empfangsbedingungen vom jeweiligen Service abhängen, werden ECM jedem Service zugeordnet. Nach dem Empfang einer ECM wird diese direkt an das Sicherheitsmodul weitergeleitet. Das Kontrollwort CW muß vertraulich übertragen werden. Zum Schutz der ECM werden kryptographische Methoden eingesetzt. Da die ECM an alle Kunden gesendet werden, müssen alle autorisierten Kunden den gleichen Schlüssel zum Entschlüsseln des Kontrollwort-Kryptogramms besitzen. Dieser wird Serviceschlüssel, SK, genannt. Das Kontrollwort CW sollte in relativ kurzen Abständen ausgetauscht werden, um das Erkennen von Scrambling-Mustern unmöglich zu machen.

Zum Setzen und zur Änderung von Empfangsberechtigungen, die im Dekoder bzw. im Sicherheitsmodul gespeichet sind, werden Entitlement Management Messages (EMM) eingesetzt. EMM-Nachrichten müssen an die individuelle Adresse des Kunden (bzw. des Dekoders oder des Sicherheitsmoduls) gesendet werden. Kundenadresse und EMM-Nachrichten müssen gegen Veränderung geschützt werden; es muß sichergestellt sein, dass nur der Programmanbieter EMM-Nachrichten erzeugen kann. Individuelle Adressen tauchen in den EMM-

Nachrichten immer unverschlüsselt auf; einen Vervielfältigungsschutz kann man nur über eine ergänzende Information erreichen, die für den Kunden unauslesbar gespeichert ist. Dies ist der persönliche Schlüssel (PK), der mit der Kundenadresse verknüpft ist. EMM-Nachrichten werden über das gleiche Rundfunksystem wie die Nutzdaten versendet. EMM-Nachrichten sind nicht fest mit dem Programminhalt verknüpft, sondern mit der logischen Adresse des Endgerätes des Kunden bzw. mit der des Sicherheitsmoduls, so dass EMM an einzelne Kunden oder an Gruppen von Kunden adressiert werden können. Für die Nutzung bestimmter Dienste wie z.B. mobil empfangene Services oder Pay-per-View kann darüber hinaus ein Rückkanal zur Verfügung stehen der entweder manuell (Anruf bei einem Service-Center) oder automatisch (z.B. Verbindung vom Dekoder zum Sendezentrum über TCP/IP) realisiert wird.

Berechtigungen können sich ändern, wenn z.B. die Gebührenkonten von Kunden nicht ausgeglichen werden, was zum Beispiel die Sperrung einer Empfangsberechtigung zur Folge haben kann. EMMs können jedoch auch dazu dienen, Dienste auf Smart Cards erstmals oder neu zu aktivieren. In diesen Fällen müssen die Berechtigungen im Sicherheitsmodul, wie Smart Card, neu gesetzt werden. Heute werden als Sicherheitsmodule meist Chipkarten verwendet, die nicht fest mit dem Endgerät verbunden sind, sondern auch aus diesem entfernt und ausgetauscht werden können.

Zum Stand der Technik wird auf die Veröffentlichung in Bernd Seiler (Hrsg.): taschenbuch der telekom praxis 1996, Schiele & Schön Berlin 1996, Jörg Schwenk: "Conditional Access" oder "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?" verwiesen.

Darüber hinaus werden mit der Einführung neuer Übertragungsmedien wie DAB und DVB-T, Pay-Dienste mit zunehmendem Maße auch für mobile Kunden, die z.B. ein entsprechendes Endgerät in ihrem Kfz mitführen, interessant. Hier stellen sich jedoch folgende Probleme:

- Die Datenkapazität der Dienste ist beschränkt (z.B. DAB, Swift u.a.),
- die Empfangssituation ist schwierig (z.B. durch noch nicht voll ausgebaute Rundfunknetze oder Kfz in Tiefgarage)) oder
- ein Rückkanal ist in der Regel nicht vorhanden.

Technische Aufgabe:

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren anzugeben, mit welchem eine Chipkarte eines autorisierten Kunden zur Änderung für Pay-Dienste individuell adressierbar gemacht werden kann, wobei die Pay-Dienste auch für mobile Kunden dienstbar gemacht werden sollen.

Offenbarung der Erfindung und deren Vorteile:

Die Lösung der Aufgabe besteht darin, dass auf Anforderung eines Service-Providers, also eine zur Ausgabe bzw. zum Verkauf von Sicherheitsmodulen berechtigte Institution, wie z.B. ein T-Punkt, an ein für die Berechtigungskontrolle zuständiges Service-Center, z.B. Daten-Service-Center im DAB, das Service-Center bei indirekter Freischaltung entweder mittels Telefon oder Datenfernübertragungssystem ein diesem Sicherheitsmodul spezifisch zugeteiltes EMM-Freischaltsignal zum Service-Provider sendet und dort dieses EMM-Freischaltsignal für den betreffenden Service in ein Kontrollgerät des Service-Providers einspeist und auf den Sicherheitsmodul aufgegeben und über das Kontrollgerät der Sicherheitsmodul mit diesem EMM-Freischaltsignal aktiviert wird oder bei direkter Freischaltung das Service-Center unter Zuhilfenahme eines Datenübermittlungsdienstes in einem digitalen Rundfunkdienst wie das DAB-Gleichwellennetz das spezifisch zugeteilte EMM-Freischaltsignal an den Sicherheitsmodul des nachfragenden Kunden sendet und diesen freischaltet. Der Erfindung liegt der Vorteil zugrunde, dass die Freischaltung eines Dienstes auf einem Sicherheitsmodul wie einer Smart Card mittels des jeweiligen Sendesystems, wie

zum Beispiel durch Nutzung handelsüblicher DAB- oder DVB-Empfänger selbst, bei direkter Freischaltung, oder unter Zuhilfenahme eines anderen als des sendenden Dienstes möglich ist bei indirekter Freischaltung. Das Service-Center vergibt die Berechtigung nach Zahlung der entsprechenden Datendienstgebühr mittels o.g. direkter oder indirekter Freischaltung über die Smart-Card-spezifische EMM. Ein beim Service Provider aufgestelltes Kontrollgerät bestätigt die Aktivierung des Sicherheitsmoduls, etwa einer Smart Card, für den betreffenden Dienst.

Bei direkter und indirekter Freischaltung kann vorteilhaft eine Zuweisung eines elektronisch gespeicherten, dienstespezifischen Guthabens, Token, in Geldeinheiten auf den Sicherheitsmodul aufgegeben werden.

Bei indirekter Freischaltung des Sicherheitsmoduls der nachfragenden Kunden kann vorteilhaft der Datenübermittlungsdienst z.B. über ein festnetzgebundenes Modem, über ein GSM-Modem oder über GSM-SMS-Dienste erfolgen.

In vorteilhafter Weise kann des Weiteren bei direkter Freischaltung des Sicherheitsmoduls des nachfragenden Kunden dieser mit Hilfe des von ihm benutzten Mobilfunknetzes, beispielsweise dem GSM-Netz, ungefähr lokalisiert werden und das spezifische EMM-Freischaltsignal zur Freischaltung des Kunden nur in das DAB-Gleichwellennetz geroutet werden, in der sich der Kunde zur Zeit des Anrufs und orderns des EMM-Freischaltsignals aufhält.

Dadurch werden die oben genannten Probleme durch die Realisierung eines Rückkanals mittels GSM gelöst. Der Ablauf hierzu sei am Beispiel DAB beschrieben:

1. Der Kunde meldet sich z.B. per GSM aus seinem Kfz beim Daten-Service-Center im DAB, um eine Freischaltung, zum Beispiel für einen einzelnen Datendienst oder für ein Abonnement oder bei Nichtempfang einer

Freischaltung oder eine Zuweisung von elektronischem, dienste-spezifischem Guthaben, Token, auf der Smart Card zu verlangen.

2. Im Daten-Service-Center im DAB wird in Zusammenarbeit z.B. mit einem GSM-Betreiber (z.B. T-Mobil) die GSM-Zelle (bzw. über diesen Weg das flächenmäßig größere DAB-Gleichwellennetz) ermittelt, in der sich der Anrufer gerade aufhält.

3. Die entsprechende EMM mit der Freischaltung wird zu dem DAB-Gleichwellennetz geroutet, in dem sich der Teilnehmer aufhält.

Die Vorteile des erfindungsgemäßen Verfahrens sind somit insbesondere darin zu sehen: EMMs müssen nicht mehr bundesweit ausgestrahlt werden, sondern nur noch lokal in den DAB-Versorgungsgebieten, in denen sich der Teilnehmer auch aufhält. Dadurch wird die für EMMs benötigte Datenrate erheblich geringer. Bei einem Anruf ist sichergestellt, daß der Anrufer die EMM auch empfangen kann, da man aus der Tatsache des Aufbaus einer GSM-Verbindung auf die Möglichkeit des DAB-Empfangs schließen kann. Ein weiterer wichtiger Vorteil besteht darin, dass ein Rückkanal für neue Dienste vorhanden ist.

Dabei werden die EMMs z.B. nicht über einen GSM-Kanal gesendet, da dies eine Datenverbindung zwischen dem Handy und dem DAB-Empfänger voraussetzen würde, was allerdings theoretisch denkbar ist.

Gewerbliche Anwendbarkeit:

Das erfindungsgemäße Verfahren ist insbesondere zur Freigabe von kunden-relevanten Zugangsberechtigungen in Conditional Access Systemen zum Empfang von gebührenpflichtigen Media-Diensten gewerblich anwendbar.

Patentansprüche

1. Verfahren zur Freischaltung von kundenrelevanten Zugangsberechtigungen in Conditional Access-Systemen zum Empfang gebührenpflichtiger Dienste, wie Pay-TV, digitale über Rundfunk ausgesendete Daten im DAB, DVB, Swift sowie Video-on-Demand, unter Benutzung von Sicherheitsmodulen, wie Smart Cards, auf welchen Sicherheitsalgorithmen und/oder kundenspezifischen Berechtigungen in Form von Softwareprogrammen und Daten gespeichert sind, **dadurch gekennzeichnet,** dass auf Anforderung eines Service-Providers, also einer zum Verkauf von Sicherheitsmodulen berechtigten Institution, an ein für die Berechtigungskontrolle zuständiges Service-Center, das Service-Center bei indirekter Freischaltung entweder mittels Telefon oder Datenfernübertragungssystem ein diesem Sicherheitsmodul spezifisch zugeteiltes EMM-Freischaltsignal zum Service-Provider sendet und dort dieses EMM-Freischaltsignal für den betreffenden Media-Dienst in ein Kontrollgerät des Service-Providers einspeist und auf den Sicherheitsmodul aufgegeben und über das Kontrollgerät der Sicherheitsmodul mit diesem EMM-Freischaltsignal aktiviert wird oder bei direkter Freischaltung das Service-Center unter Zuhilfenahme eines weiteren Datenübermittlungsdienstes in einem digitalen Rundfunkdienst das spezifisch zugeteilte EMM-Freischaltsignal an den Sicherheitsmodul des nachfragenden Kunden sendet und diesen freischaltet.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass bei direkter und indirekter Freischaltung eine Zuweisung eines elektronisch gespeicherten, dienstespezifischen Guthabens (Token) in Geldeinheiten auf den Sicherheits-modul aufgegeben wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass bei indirekter Freischaltung des Sicherheitsmoduls des nachfragenden Kunden der Datenübermittlungsdienst wahlweise über ein festnetzgebundenes Modem, ein GSM-Modem, oder über GSM-SMS-Dienste erfolgt.

4. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass bei direkter Freischaltung des Sicherheitsmoduls des nachfragenden Kunden dieser mit Hilfe eines digitalen Mobilfunknetzes ungefähr lokalisiert wird und das spezifische EMM-Freischaltsignal zur Freischaltung des Kunden nur in das digitale Rundfunknetz geroutet wird, in der sich der Kunde zur Zeit des Anrufs und Order des EMM-Freischaltsignals aufhält.

Zusammenfassung

Verfahren zur Freischaltung von kundenrelevanten Berechtigungen auf Sicherheitsmodulen in Conditional Access Systemen für Pay-Dienste

Die Erfindung betrifft ein Verfahren zur Freischaltung von kundenrelevanten Zugangsberechtigungen in Conditional Access Systemen zum Empfang von gebührenpflichtigen Media-Diensten unter Benutzung von Sicherheitsmodulen, wie Smart Cards, auf welchen Sicherheitsalgorithmen und/oder kundenspezifischen Berechtigungen in Form von Softwareprogrammen gespeichert sind. Auf Anforderung eines Service-Providers, wie z.B. ein T-Punkt oder eine andere zum Verkauf von Sicherheitsmodulen berechtigte Institution, sendet ein für die Berechtigungskontrolle zuständiges Service-Center bei indirekter Freischaltung entweder mittels Telefon oder Datenfernübertragungssystem ein diesem Sicherheitsmodul spezifisch zugeteiltes EMM-Freischaltsignal zum Service-Provider, wo dieses EMM-Freischaltsignal für den betreffenden Media-Dienst in ein Kontrollgerät des Service-Providers einspeist und auf den Sicherheitsmodul aufgegeben wird und über das Kontrollgerät der Sicherheitsmodul mit diesem EMM-Freischaltsignal aktiviert wird. Bei direkter Freischaltung sendet das Service-Center unter Zuhilfenahme eines weiteren Datenübermittlungsdienstes in einem digitalen Rundfunknetz wie das DAB-Gleichwellennetz das spezifisch zugeteilte EMM-Freischaltsignal an den Sicherheitsmodul des nachfragenden Kunden und schaltet diesen frei.